



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,676	11/26/2001	Po-Tong Wang		4163
7590	03/24/2005			
Po-Tong Wang PO Box 82-144 TAIPEI, TAIWAN			EXAMINER POLTORAK, PIOTR	
			ART UNIT 2134	PAPER NUMBER

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/991,676	Applicant(s) WANG, PO-TONG	
	Examiner Peter Poltorak	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 November 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

tu

DETAILED ACTION

1. Claims 1-5 have been examined.

Claim Objections

2. Claims 1-3 are objected to. The claims use the following terms:

- a. Claim 1: KDC,
- b. Claim 2: IC and 2D
- c. Claim 3: BIR

The terms are not well defined in the specification and as such provide some level of uncertainty as to the intended meaning. The examiner suggests amending the terms to more clearly identify intended limitations, e.g. Key Distribution Center (KDC), integrated circuit (IC), 2-Dimensional (2D), Biometric Information Record (BIR) etc.

Also, if the applicant indeed referred to the Key Distribution Center as the KDC the examiner suggests using recitation "stored in said KDC" instead of "stored on said KDC".

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 5 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not

Art Unit: 2134

described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claims recite limitations directed towards International Biometric Industry Association (IBIA); however, no documentation is provided.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-5 are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.
5. Claims 1-5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.
6. In claim 4 the "said computer chip means" lacks antecedent basis.
7. Claim 1 is ambiguously written:
 - a. The term "physical immutable identification credentials of a user" is not understood. It is unclear for example whether a card with a picture and a magnetic strip would satisfy the limitation.
 - b. Applicant uses the terms means for:
 - "providing high security of transmission" is not understood.
 - "comparison"
 - Transmitting

Art Unit: 2134

- Comparison
- Approval

but no explanation on the terms is provided in the specification.

- c. The term “activated biometric features” is not understood.
- Similarly, the term “digitized BIR” is not understood and as a result the distinction between the “digitized BIR” and the “activated biometric features” which is stored on KDC is ambiguous.
- d. Claim 1 is a method claim but in addition to method steps it recites capabilities, “encrypting means for using a public key of KDC to encrypt data”.
- e. The term “using the DES algorithm from a user’s host” is not understood. Although the limitation is assumed to be addressed to a computing device of a user it is unclear whether the algorithm is downloaded from “a user’s host”, or whether the limitation implies that the DES algorithm is used on the user’s host or something else.
- f. The claim language recites: “to perform verification by collation and comparison”. It is not clear what is verified: data, the cryptographic key, biometric verification, all of the above or something else.
- g. The limitation: “comparing said decrypted key with the original stored numbers” is not understood.
- h. The term: “releasing the user’s private key” is not understood.
- i. “Overcoming the need to carry, store or remember private keys” is not understood. The specification does not clearly define the term and the only way

Art Unit: 2134

the need can be overcome is by a computer not getting in contact with the key.

Processing (including reading, sending etc.) utilizes a computing device

memory which would read on "carrying, storing or remembering". Furthermore,

it is not clear what subject the limitation refers to: e.g. user's host, KDC, both, or

something else. The limitation is especially confusing since dependt claim 3

suggests: "storing the private key of the user in a computer chip".

8. Claim 2 is phrased grammatically incorrect. As a result it is not clear whether the limitation refers to the user's host comprising specified attributes (e.g. bank card, a credit card etc.) or whether the sentence is missing the end limitation.
9. Claim 3 recites: "Performing the BIR process and encryption/decryption processes of the user". The language as cited suggests that the user is encrypted/decrypted. Also it is not clear to which processor the limitation refers: the user's host or KDC. Clarification is required.
10. The capitalization of letters: "Storing" and "Performing" in claim 3 is not understood. There are no bullets and no periods to justify the capitalization.
11. Claim 4 is ambiguous and the limitations as cited are difficult to understand both in part and as a whole. Also, the claim as written seems to be incomplete.
12. Claim 4 recites: "said computer chip means for comprising RISC CPU, CISC CPU, DSP, FPGA, CPLD, NET ASIC, Microprocessor, Micro controller and other chips with function calculation". The recitation "chip means" (discussed above) is not defined in the specification. Similarly, "chips means for comprising system on-a-

Art Unit: 2134

chip, system-on-multiple-integrated-chips and system-on-multiple-chips" is not understood.

Furthermore the language is ambiguous. It is not clear whether the intended meaning is to provide one of the microprocessors listed, all of them or perhaps the limitation suggests providing the processors with function calculations.

Also, the limitation introduces a computer jargon with no clear definition in the claims nor in the specification. As a result, the distinction between some of the terms, e.g. CISC CPU and Microprocessor is unclear.

13. Claim 4 appears to be incomplete and leaves no room to deduce what "the elements of said chips means for comprising system-on-a-chip (SOC), system-on-multiple-integrated-chips and system-on-multiple chips" should do or have.

14. As per claim 5 the "biometric characteristics means" is not understood.

Furthermore, the claim seems to be incomplete. As a result it is not clear whether the claim language recites examples of biometric characteristics, all of the characteristics that must be present in a device (if so, not clear what device), at least one of the characteristics must be present in a device or something else.

15. The term "according to the standard of IBIA" is not understood. The scope of the standards may change over time and the specification did not provide any documentation, that clearly sets the metes and bounds of the claim's limitation.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

Art Unit: 2134

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. Claims 1 and 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Spies et al.* (U.S. Patent No. 6230269) in view of *Tomko* (U.S. Patent No. 5790668) and in further view of *Schneier* (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457).

17. As per claim 1 (as best understood) *Spies et al.* teach a client authenticating to a server's system, the client generating a session key, and encrypting data (a message) with the server's private key, wherein the server authenticates a client, and server sends a public/private key pair to the client, and wherein the public/private key pair is associated with the client, encrypted with the session key and the client decrypts the receipt using the session key (col. 2 line 52 – col. 3 line 14).

This reads on utilizing identification credentials of a user to perform authentication in conjunction with cryptography technology, and means for providing high security of transmission, generating a cryptographic key of the user encrypting means for using a public key of KDC to encrypt data including said cryptographic key; Transmitting means for transmitting said encrypted data from said host to said KDC for decryption; wherein decrypting said encrypted data using a private key of KDC to

Art Unit: 2134

perform verification by collation and comparison; wherein approval means for getting approved from said verification, and for releasing the user's private key from said KDC, encoding the private key using the cryptographic key for transmitting to said host, retrieving the private key from said KDC, and for decoding the private key using said cryptographic key.

18. *Spies et al.* do not teach utilizing physical immutable identification credentials, collating biometric features, digitized BIR stored on the KDC.

Tomko teaches biometric representation being encrypted utilizing physical immutable identification credentials, collating biometric features, encrypting and decrypting biometric data and storing digitized BIR (*Tomko*, col. 2 lines 26-49).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize physical immutable identification credentials, collating biometric features, encrypting and decrypting biometric data and storing digitized BIR as taught by *Tomko*. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase security by user authentication (*Tomko*, col. 1 lines 12-32).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize physical immutable identification credentials, collating biometric features, digitized BIR stored on the KDC as taught by *Moussa et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to increase security of the system (e.g. assure a more reliable user authentication).

Art Unit: 2134

19. *Spies et al.* do not explicitly teach generating a cryptographic key using the DES algorithm.

Schneier teaches generating a cryptographic using the DES (*Schneier*, pg. 175 "DoD Key Generation" section). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to generate a cryptographic key using the DES. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase security of the key.

20. The limitations of claim 3 (*as best understood*) are implicit in light of the limitations of claim 1. In regard to a computer chip storing the private key the computer chip is necessary for processing any calculation data (e.g. the BIR and encryption/decryption) such as the received private key; in order for the data to be processed it must be stored in the chip.

21. As per claim 4 (*as best understood*) a microprocessor is necessary for functions such as encryption/decryption for example.

22. Fig. 4 in *Tomko's* teaching reads on claim 5 as best understood.

23. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Spies et al.* (U.S. Patent No. 6230269) in view of *Tomko* (U.S. Patent No. 5790668) and *Schneier* (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457) and in further view of *Official Notice*.

24. *Spies et al.* in view of *Tomko and Schneier* teach a cryptography method as discussed above.

Art Unit: 2134

25. As per claim 2 (as best understood) *Spies et al.* in view of *Tomko and Schneier* do not explicitly teach host means for comprising a bank card, a credit card, a storage valued card, a magnetic strip card, an IC card, a smart card, an optical card, a CD, a DVD, a 2D bar code card, a portable magnetic storage device, a portable electronic memory device and a portable mobile storage device.

26. Official Notice is taken that it is old and well-known practice to include a CD, DVD or other above described devices within a user's host to take advantage of alternative data providing and reception.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent


Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Signature



Date

3/18/05


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100